STAT

Executive Officer
Intelligence Community Staff

See comments.

[redacted]

[redacted]

[redacted]

Chm, IHC

Please prepare comments on the attached, in coordination with Ruth Davis as appropriate, for discussion with D/ICS + DD/ICS early next week.

ILLEGIB

[redacted]

Thanks

[redacted]

6/14

STAT

[redacted]

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
FOR COMMAND, CONTROL, COMMUNICATIONS
AND INTELLIGENCE

Date 10 June 1985

Memo for John McMahon
[redacted] 25X1

This is a very serious indictment of the safeguards document. We should discuss.

Don

Donald C. Latham

Attachment

SECRET

cc: Mr. Hawkins

UNCLASSIFIED WHEN
ATTACHMENTS ARE DETACHED

25X1

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

[redacted]

30 May 1985

WKO 3 June

DCI/IC 85-5383

MEMORANDUM FOR THE ASSISTANT SECRETARY OF DEFENSE C3I

SUBJECT: Director of Central Intelligence Memorandum NFIC-9.11/1 dated 22 Jan 85 - INFORMATION MEMORANDUM

The DoD Computer Security Center has reviewed the document "UNIFORM SAFEGUARDS FOR PROTECTION OF 'CRITICAL SYSTEMS' PROCESSING INTELLIGENCE INFORMATION". We thank you for the opportunity to review this document and to provide what we believe are important comments. Specific comments are given in the enclosure. General comments follow:

This document has several flaws, chief of which is the allowing of multilevel mode operation without secure systems. The document states that it is not necessary to implement security-related software in the operating system. Therefore, the highest class of system that would be produced using this document would be a B1, according to the Department of Defense Trusted Computer System Evaluation Criteria (hereafter referred to as the Criteria). Further, this document implies that it is permissible under certain circumstances to operate the system in multilevel mode with users possessing a wide range of clearances. Because the maximum achievable evaluation class is a B1, most critical systems should NEVER be allowed to operate in multilevel (or compartmented) mode with users possessing a wide range of clearances. [redacted] [redacted]

25X1

If this document were to be implemented as written, it would result in the Intelligence Community having a false sense of security about its critical systems. This could then result in a lessening of the effort currently underway to encourage development of truly secure systems.

This document contradicts much of the guidance that the Center has promulgated in the Criteria. It quotes some passages directly from the Criteria without ever citing the Criteria. In so doing, it distorts the intent of the Criteria in some places. The SAFEGUARDS document should be changed to be consistent with the Criteria.

25X1

[redacted]

THIS DOCUMENT MAY BE
DECLASSIFIED UPON
REMOVAL OF ENCLOSURE

SECRET

5-321

Parts of this SAFEGUARDS document are very misleading. For the past three years, the terms "mandatory access control" and "discretionary access control" have consistently been interpreted to mean that access decisions are made by the Trusted Computing Base (TCB) of the system. This document uses the terms to indicate that some access decisions are made through environmental and administrative mechanisms. If the document is going to discuss both hardware/software mechanisms and environmental/administrative mechanisms, it must make this distinction clear from the beginning. One suggestion would be to use different terminology for hardware/software controls than is used for environmental/administrative controls.

As written, this document implies that no existing "Critical System" can ever be enhanced above a B1 level. (For example, the topic of covert channels, which first appears in the Criteria at the B2 level, is not addressed at all.) The Center agrees with this assessment, and believes that this point should be explicitly stated. Further, the Center's current guidance indicates that D systems may only be used in dedicated mode, C systems may only be used in system high or dedicated mode, and B1 systems may only be used in a few multilevel and compartmented environments, along with system high and dedicated mode. Therefore, there is an implicit mapping between the levels suggested in the SAFEGUARDS document and the Criteria evaluation classes. The Center believes that this mapping should be stated explicitly in the document.

In summary, the Center believes that: (1) the SAFEGUARDS document has major flaws that must be addressed before it is issued; (2) this document should be changed to be consistent with the Criteria; and (3) if implemented as currently written, this document would allow multilevel operation of unsecure systems.

[redacted]

25X1

Assistant Director
for
Computer Security

Encl:
a/s

[redacted]

ILLEGIB

SECRET

Next 2 Page(s) In Document Denied